ARTÍCULOS

CLOUD LAW AND CONTRACT NEGOTIATION

Charles Oppenheim

Charles Oppenheim was, until he retired in 2009, professor of information science at *Loughborough University*, and is currently a visiting professor at *Queensland University*. In his past life, he has held a variety of posts in academia and the electronic publishing industry, working for *International Thomson*, *Pergamon* and *Reuters* at various times. He has been involved in, given talks on, provided consultancy services on, and published widely on the legal issues involved in the creation, dissemination and consumption of information –especially intellectual property rights, licences, data protection and freedom of information- since the mid 1980s. He is a member of the *European Commission*'s *Legal Advisory Board*.

c.oppenheim@btinternet.com

Abstract

The main characteristics of cloud computing services are explained and the clauses typically included in contracts between suppliers and customers of such services are discussed. Storing data on a cloud service can be more comfortable for an organization and cheaper than local storage, but it involves several risks. Recommendations are given on how to negotiate contracts. A list of questions to be asked of cloud service suppliers is provided so that a potential client can take an informed decision and avoid unpleasant surprises.

Keywords

Cloud computing, Contracts, Conditions, Negotiation, Features, Legal, Law, Patriot act, Risks, Privacy, Data protection, Copyright, Outsourcing, Recommendations, Relaciones proveedor-cliente.

Título: Legislación sobre computación en la nube y negociación de contratos

Resumen

Se explican las características de los servicios de computación en la nube y se discuten las cláusulas que suelen incluir los contratos entre proveedores de dichos servicios y clientes. Mantener los datos en un servicio en la nube puede ser cómodo y más barato que en una instalación local de la propia organización, pero comporta varios riesgos. Se dan recomendaciones sobre cómo negociar los contratos, y se ofrece una lista de preguntas para obtener información del proveedor y así poder tomar una decisión bien informada que evite posteriores desagradables sorpresas.

Palabras clave

Computación en la nube, Contratos, Condiciones, Negociación, Características, Aspectos legales, Leyes, Patriot Act, Riesgos, Privacidad, Protección de datos, Derecho de autor, Copyright, Externalización, Recomendaciones.

Oppenheim, Charles. "Cloud law and contract negotiation". *El profesional de la información*, 2012, septiembre-octubre, v. 21, n. 5, pp. 453-457.

http://dx.doi.org/10.3145/epi.2012.sep.02

Introduction

A cloud computing service is one that provides computing power without the installation of content, hardware or software application at the client or customer's premises.

Wikipedia defines cloud computing as follows:

"Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

Cloud computing describes a new consumption, and de-

Nota: Este artículo puede leerse traducido al español en:
http://www.elprofesionaldelainformacion.com/contenidos/2012/septiembre/02_esp.pdf

Article received on 18-01-12

livery model for IT services based on internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location; in other cases, entire business applications have been coded.

Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies."

Services such as *Facebook*, *Rackspace*, *Hotmail*, *Twitter*, *Yahoo!*, *YouTube*, *Flickr*, *eBay*, *Google Apps* (and all its subsidiary offerings such as *Gmail* and *Google Drive*), *Amazon EC2*, *TripAdvisor* and *DropBox* either employ or offer cloud services.

Interest in the use of cloud services is growing and is very understandable. Cloud services offer a cheap and efficient method of outsourcing computerised handling of all types of data to organisations that find such tasks burdensome, expensive or beyond their technical capabilities.

Cloud services and their contracts

Clients of cloud services providers (CSPs) sign up to a contract. The contracts that most cloud services offer are in general non-negotiable. It's a case of take it or leave it. Only very large or prestigious organisations will have the necessary influence to require a CSP to accept amendments to its standard terms and conditions. There have been a number of surveys carried out of cloud service contracts; these have demonstrated that many of the standard contracts are extremely one-sided in favour of the cloud supplier. A typical one-sided example comes from *Apple*'s *iCloud service*:

> "You acknowledge and agree that *Apple* may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as *Apple* believes is reasonably necessary or appropriate, if legally required to do so or if we have a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of *Apple*, its users, a third party, or the public as required or permitted by law."

If an individual or small organisation doesn't like the standard terms offered, it has to make a decision whether to risk accepting the standard contract, try another cloud supplier, or give up on cloud services altogether.

Very few cloud service contracts offer guarantees of good service (e.g., 100% uptime), and those that offer refunds for poor service availability typically offer such refunds in terms of money off a future renewal of the subscription rather than a refund of the existing subscription. So if the client is so annoyed by poor availability it decides to not renew, or to cancel its current contract, it will get no refund for the problems encountered. Some contracts give the service supplier the right to close the service at little or no notice. Presumably it would only do this if the service was unprofitable or if the cloud service supplier itself was in serious financial difficulty, but the danger is that the client who depends on the service for its day-to-day business activities may be left suddenly in great difficulty.

Overall, the contracts tend to put what few obligations there are on the clients rather than on the service supplier. Few offer automatic encryption of data given to them and/or anonymisation of personal data. In recent years, the concept of a privacy impact assessment (PIA), i.e., an independent assessment of the risks to privacy of a particular service or system, together with advice on how to tighten things up if necessary, has become popular. Few of the cloud contracts include references to PIAs. They also do not give clients the ability to check privacy compliance.

Many cloud service suppliers include a clause by which they exclude all liability for any problems that arise in the service, whether or not it was caused by the service supplier's incompetence or recklessness. The legality of such clauses is unclear, especially when imposed on an individual. It is reasonable to suggest that such clauses, which indicate an immaturity of, and lack of confidence in, the cloud service supply industry.

> "Some service suppliers' clauses excluding liability indicate an immaturity of, and lack of confidence in, their industry"

Most business users of cloud services will no doubt have some form of notice and take down policy and procedures on their Web sites, explaining how any third party can complain about content on its Web site (e.g., it infringes copyright or is defamatory). What if a cloud service supplier maintains that Web site? The service contract should address the question of how rapidly the cloud supplier can take down offending materials if the client asks it to, but most cloud contracts do not address this issue.

A CSP will no doubt wish to monitor use to assess bandwidth and hardware use, for statistical analyses, business planning etc., and indeed some of these statistics could be useful for the client as well. The potential cloud service client should examine the contract terms carefully to ensure that they clearly explain the monitoring carried out, and that it is content with whatever monitoring occurs.

The contract should also outline the procedures with respect to deletion of data if and when the contract with the CSP ends. The client will want to know whether the cloud provider will delete their data on termination. It is likely that the client will want all copies of data in the possession of the cloud provider deleted after it has exercised its rights to have data returned. And, of course, it will want to ensure that the data is returned in a format that is appropriate for any future use made of that data.

Data protection and security issues in the cloud

Almost by definition, data stored in the cloud will move from country to country, each with its own laws. In addition, the CSP may well be based in a different country to that of its clients. The situation becomes particularly problematic when considering the legality of the contract, such as the differing requirements for "fairness" in different countries. There are potentially at least four countries' laws to consider in the case of personal data stored in the cloud – the home base of the service supplier, the home base of the client, the country in which an individual whose information is stored is based, and the country where the cloud happens to be residing at any given time. Questions then arise regarding liability should, say, personal data leak out in some unauthorised way. Even if there is no personal data present, three countries' laws (the home base of the service supplier, the home base of the client and the country where the cloud happens to be residing at any given time) may apply to any actions taken with the data or any legal cases arising from the contract.

> "Data provided to a cloud service supplier can move from country to country without the client knowing when or where"

Numerous surveys of users, and potential users of cloud services have demonstrated concerns about the security of data, e.g., hacking, as well as data protection/privacy concerns as potential inhibitors to the use of cloud services. The key risks are seen as the exposure of confidential and personal information to governments, competitors, thieves or opportunists.

The cloud's ubiquitous and dynamic nature means that data provided to a cloud service supplier will move from country to country without the client knowing when or where the data is being moved. Furthermore, the data might well be backed up or replicated in multiple countries. Indeed, it is possible that more than one CSP will co-operate and transfer data between their servers. However, data protection (and other) laws vary greatly from country to country, with some countries offering no realistic protection at all in their legislation. Ideally, then, the contract between the CSP and the client should cover questions of who is responsible for ensuring that personal data is kept safe. Furthermore, the contract should include provision for the CSP to pay compensation to individuals, or any fine should a breach of any Data Protection legislation result from the CSP's own failings. In addition, many Data Protection Acts provide an official regulator with the powers to impose notices requiring the data owner to do something, or to supply certain information. The contract must ensure that the cloud service responds rapidly to either requirement.

Many countries' data protection legislation make it illegal to transfer personal data to a country without adequate data protection laws unless the transfer is necessary for a contract, has the explicit approval of the individual, or for a few other restricted reasons. Most CSPs are US-based, though some have EU-based subsidiaries. Those that are US-based often commit to Safe Harbour Principles, i.e., that data in their care will be placed in a physical environment where EU data protection laws are followed. However, not all commit to this, and it would be a very strange cloud service that committed to never letting data under its control outside the European Economic Area. Those that do not commit to a Safe Harbour are therefore particularly high risk from a client's point of view, as the data may well be held in a country with little or no regard for data protection laws. Rather worryingly, some of the biggest CSPs do not commit in their contracts either to follow EU data protection laws, or to place client data in a safe harbour. Furthermore, the contracts do not oblige the CSP to inform a client if a search warrant has been issued to inspect the data it holds.

Even if the CSP promises to maintain the data it is entrusted with in a safe harbour, how can one be sure the data will always stay in a safe harbour when the entire business rationale for cloud is to place the data in whatever is the economically most advantageous place? The data will be kept in whatever data centre is available, and may only stay there a short time before being moved on to another data centre. One approach to this potential problem is to get the CSP to agree to use a safe harbour combined with a "if anything goes wrong you will be subject to the rules of the EU data protection law" contractual obligation. Then, if anything did go wrong, the supplier would be penalised as if they were operating within the EU. But, as noted above, CSPs are notoriously unwilling to negotiate on contractual terms. Nonetheless, it is strongly recommended that a potential client demand that basic safe harbour principles be applied.

Patriot act

One particular area of concern is the *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism*, better known as the *Patriot act*. This wide-ranging piece of legislation allows US authorities to compel, amongst others, internet service providers (ISPs) and cloud service providers to disclose information about their customers and/or the data stored or used by those customers, and without those customers knowing that such information has been requested. Despite the *Act*'s title, its use can extend beyond terrorism to many other types of criminal investigation. Because of its wide-ranging powers, this *Act* has been viewed with distaste by those countries with well developed data protection legislation in place, and has led to some governments (e.g., Canada and Netherlands) banning organisations under their con-

trol from passing any data to US-based organisations, and has allegedly led to *Amazon* delaying the launch of its new *Kindle Fire* within the EU because of the incompatibility of the *Patriot act* with EU data protection legislation.

The key issue for a cloud service client, therefore, is not just whether the cloud service offers a safe harbour for its information, but also whether it wishes to take the risk that its data might end up in the hands of US authorities as a result of a *Patriot act* action. An informed judgement should be made, and I recommend great caution be exercised if the data is particularly sensitive, either in terms of personal data, or in terms of commercially confidential data. It is one of many risk factors one should take into account when engaging a cloud service supplier. The *Patriot act* is not alone of course; there are similar pieces of legislation in other countries where cloud data might be held, but they are generally not as far-reaching or as well known as the *Patriot act*.

Security

Security issues are also a major concern. There have been anecdotal reports of instances when one cloud service client was able to read another cloud service client's materials for short periods of time. A prospective client of a cloud service therefore should undertake appropriate due diligence about the cloud service it is thinking of using to assure themselves that security is at a level appropriate to the value and/or sensitivity of the information which may be passed to that cloud service. It is also a good idea to test the cloud service first with non-sensitive information. I recommend that the contract with the CSP be negotiated if possible to include a clause obliging the service to comply with certain specified international security standards, and/or with the client's own security standards. The contract should make explicit the service provider's liability (and limits of liability) in case of data loss or a security breach. Clients should resist any contract that absolves the cloud service from any liability for data loss or security breach.

Other legal issues

Data protection and security of data are not the only legal issues that can arise. Questions might arise regarding who is responsible if the data offered by a client are somehow amended or released resulting in an illegality, such as defamation or breaking national security laws. It is not clear what country's laws might apply in such cases. Whilst it is unrealistic to expect the CSP to monitor everything on its servers (and indeed, this could be problematic from a privacy point of view), it is reasonable to expect it to respond to complaints received regarding alleged defamatory comments. The contract or a Service Level Agreement between the client and the CSP will probably include warranties and instructions relating to alleged defamatory statements or other potentially illegal materials stored on the cloud's servers.

Software licences, copyright licences and database rights licences are also –and somewhat surprisingly- potentially problematic. If a client has permission to use a particular software or database "on site", does that include "in the cloud"? A licence might state that the material must not be sent to another country. Such restrictions may even go further, stating that a particular database or software may only be used on a single computer, or may only be used by employees of the licensee. If such databases and/or software are going to be placed in the cloud, these database or software licences will have to be renegotiated. Many database and software licensors are aware of the cloud and are willing to be flexible on this matter. If they are not, then a decision has to be taken whether to place that database/software on the cloud, or to use an alternative database/software that imposes no such restrictions.

Finally, client service clients should ensure that the contract confirms that the ownership of copyright and other Intellectual Property Rights in materials passed by the client at any time to the service remain with the original owners, and is not assigned to the cloud service.

Questions to ask a cloud service supplier before you sign up

I suggest below a list of questions that could be asked of any CSP before signing its contract:

- Who (both within and outside the service supplier) will be able to see my information?
- Who owns and controls your infrastructure? Is this outsourced to any third party?
- Where are the infrastructure elements located? (Then check what data protection laws apply in those countries; if the answer is "it is not known in what countries the data might be held", it is best not to sign up to that cloud supplier)
- Can I see a copy of your reliability/availability/downtime reports (if any)?
- What service levels are guaranteed, e.g., availability, time taken to resolve a problem, and what compensation do you offer if you fail to fulfil that? (In particular, would-be clients should resist the current standard practice of discounts on future subscriptions, but insist where possible to receive financial compensation there and then and/or the right to terminate early with refunds)
- Have you ever had security breaches in the past? (If "yes", ask for more details.)
- Do I have a contact name within your organisation in case of any problems?
- Will you abide by the local relevant Data Protection Act (if one applies) when you handle my information? Will you pay damages if a breach of the Act occurs which is your fault? What assurances can you give that data protection standards will be maintained even if the data we supply is stored in a country with weak, or no data protection laws, or where government inspection powers are very wide-ranging?
- How easy would it be to migrate my data to a competitor service once this contract ends? Can you guarantee that it will be in a usable format?
- Who is responsible for ID management and access control in your company?
- What are the names of your employees responsible for handling our data?

- What security policies, technology and systems do you employ? What national or international standards do they comply with?
- Do I get any rights of refusal before you make changes to the service that affect my data? (Alternatively, can we cancel early and get money back if we cancel early because of unwanted service changes?)
- Will you use my organisation's name or type of data given to you on any of your advertising? (If need be, require that the cloud supplier has to ask for permission each time)
- What special measures will you take regarding data we tag as confidential?
- Could we have a free trial with some non-sensitive data before committing ourselves?
- Are you willing to include clauses in the contract relating to ensuring there is no unauthorised loss or destruction of data?
- Can you provide us with routine backups of all our data stored on your cloud?
- Will you guarantee to inform us if you become aware of any data security breach that affects or involves our data?
- Finally, and most important, is your contract negotiable?

Some of these questions may well be answered in the draft contract, in documents published by the service or in informal discussions with cloud service sales executives. Some of the answers you should press to be included in the contract itself or in a Service Level Agreement, i.e., you should not allow yourself to be satisfied with informal assurances. The real issue in using cloud services is that you are entering into a relationship on standard terms and conditions, with little power to negotiate. You need faith in the provider to be comfortable with that position. The types of answers (or the refusal to provide answers) to the questions above should help inform you on that faith.

I would conclude that one should not get paranoid about the cloud. It offers many potential benefits. But one should enter into a cloud contract being aware of both the benefits and the risks and should make an informed risk assessment before committing you, or your employer, to a cloud service.

Some recent bibliography and resources

Carlton, Gregory H.; **Zhou, Hill**. "A survey of cloud computing challenges from a digital forensics perspective". *Intl Journal of Interdisciplinary Telecommunications and Networking*, 2011, v. 3, n. 4, pp. 1-16.
http://dx.doi.org/10.4018/jitn.2011100101

Cheng, Fa-Chang; **Lai, Wen-Hsing**. "The impact of cloud computing technology on legal infrastructure within internet-Focusing on the protection of information privacy". *Intl workshop on information and electronics engineering, Procedia engineering*, 2012, v. 29, 2012, pp. 241-251.
http://dx.doi.org/10.1016/j.proeng.2011.12.701

González, Nelson; **Miers, Charles**; **Redigolo, Fernando F.**; **Carvalho, Teresa C.**; **Simplicio, Marcos A.**; **Naslund, Mats**; **Pourzandi, Makan**. "A quantitative analysis of current security concerns and solutions for cloud computing". En: *IEEE 3rd intl conf on cloud computing technology and science (CloudCom)*, Nov. 29 2011-Dec. 1 2011, pp. 231-238.
http://dx.doi.org/10.1109/CloudCom.2011.39

Hay, Brian; **Nance, Kara**; **Bishop, Matt**. "Storm clouds rising: security challenges for iaas cloud computing". En: *44th Hawaii intl conf on system sciences (Hicss)*, 4-7 Jan. 201, pp. 1-7.
http://dx.doi.org/10.1109/HICSS.2011.386

Inteco-Cert. *Riesgos y amenazas del cloud computing*. Madrid: Instituto Nacional de Tecnologías de la Comunicación; Mº de Industria, Turismo y Comercio; Plan Avanza 2; marzo 2011, 32 pp., 489 KB
http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Klein, Carolina A. "Cloudy confidentiality: clinical and legal implications of cloud computing in health care". *J Am Acad Psychiatry Law*, 2011, v. 39, pp. 571–578,
http://www.jaapl.org/content/39/4/571.full.pdf+html

Legal Cloud Computing Association
http://www.legalcloudcomputingassociation.org

Mell, Peter; **Grance, Timothy**. *The NIST Definition of Cloud Computing. Special Publication 800-145*. Computer Security Division, Information Technology Lab., National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, Sept. 2011, 7 pp.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

National Archives of Australia. *Records management and the cloud - a checklist*, 2011, 5 pp., 444 KB
http://www.naa.gov.au/Images/Cloud_checklist_with_logo_and_cc_licence_tcm16-44279.pdf

Schweitzer, Eugene J. "Reconciliation of the cloud computing model with US federal electronic health record regulations". *J Am Med Inform Assoc*, 2012, v. 19, pp. 161-165.
http://dx.doi.org/10.1136/amiajnl-2011-000162
http://jamia.bmjjournals.com/content/19/2/161.full.pdf+html

Wood, Katie; **Anderson, Mark**. "Understanding the complexity surrounding multitenancy in cloud computing". En: *IEEE 8th Intl Conf. on e-Business Engineering (Icebe)*, 19-21 Oct. 2011, pp. 119-124.
http://dx.doi.org/10.1109/ICEBE.2011.68